# COUNCIL ON FOREIGN RELATIONS

58 EAST 68TH STREET • NEW YORK • NEW YORK 10021
Tel 212 434 9400 Fax 212 434 9875


**"The Continued Vulnerability of the Global Maritime Transportation System"**

Written Testimony before

a hearing of the

Subcommittee on Coast Guard and Maritime Transportation
Committee on Transportation and Infrastructure
United States House of Representatives

on

"Foreign Operations of U.S. Port Facilities"

by


Stephen E. Flynn, Ph.D.
Commander, U.S. Coast Guard (ret.)
Jeane J. Kirkpatrick Senior Fellow in National Security Studies
sflynn@cfr.org


Room 2165
Rayburn House Office Building
Washington, D.C.

9:30 a.m.
March 9, 2006

**"The Continued Vulnerability of the Global Maritime Transportation System"**

by
Stephen E. Flynn
Jeane J. Kirkpatrick Senior Fellow
for National Security Studies

Chairman Lobiondo, Ranking Member Filner, and distinguished members of the House Subcommittee on Coast Guard and Maritime Transportation. Thank you for inviting me this morning to discuss the federal government's progress in implementing maritime security measures as required by the Maritime Transportation Security Act of 2002 and my recommendations of how to advance this critical agenda.

The controversy surrounding the takeover of five American container terminals by Dubai Ports World has had the salutary benefit of engaging Washington and the American people in a national conversation on the state of port security. This is long overdue given the enormous national security and economic security stakes should the next catastrophic terrorist attack on U.S. soil involve the global maritime transportation system and America's waterfront. While it has too often been lonely work, Chairman Lobiondo, I commend you and your committee for your leadership in advocating that our critical maritime infrastructure should not be overlooked in our post-9/11 efforts to secure the American homeland.

This is my second opportunity to appear before this committee. On August 25, 2004, I provided testimony that I entitled "The Ongoing Neglect of Maritime Transportation Security." At the hearing I said: "I believe maritime transportation is one of our nation's most serious vulnerabilities, and we are simply not doing enough to respond to the terrorist threat to this critical sector." Sadly, I have seen too little progress in the ensuing 18 months to modify that assessment. Based on my visits to a dozen major seaports within the United States and abroad since 9/11, my conclusion is that the security measures that are currently in place do not provide an effective deterrent for a determined terrorist organization intent on exploiting or targeting the maritime transportation system to strike at the United States.

At the federal level, the primary frontline agencies—the Coast Guard and Customs and Border Protection Agency—are grossly under-funded for what essentially became a new major mission for them on 9/11. On the local and state levels, the size of port authority police forces remain tiny, providing often only token police presence within most seaports. While the Maritime Transportation Security Act of 2002 represented a constructive stepping off point for advancing security within this sector, we have made little meaningful progress since then.

In my remarks today, I will speak to both the shortfalls in our port security efforts within the United States and with our efforts to advance port security overseas, and will provide some recommendations on how we should proceed. Our domestic and international efforts must be complementary because seaports, at the end of the day, are simply onramps and offramps into a global transportation network. To focus on just the security

of U.S. seaports is a bit like a computer network security manager who only puts in place firewalls for the computers within reach of his desk. If the whole network is not secure, such an effort will be futile.

To begin with, we must candidly acknowledge that MTSA is more of a sketch than a security blueprint; that is, it sets forth general requirements without establishing minimum standards for satisfying those requirements. For instance, the MTSA requires vessels and marine facilities have a plan for establishing and maintaining physical security, passenger and cargo security, and personnel security. However it does not define what that security is. It requires that there be a system for establishing and controlling access to secure areas of the vessel or facility, but it does not elaborate how that should be done. It mandates that there be procedural security policies, but provides no guidance on what those policies should be. MTSA requires that there be a "qualified individual" to implement security actions, but sets no standards on what it takes to be "qualified." There are not even any minimal training standards. The Coast Guard has worked with the Maritime Administration to create a "model" training course, but there is no requirement that facility or ship security officers attend a certified course base on this model curriculum.

The International Maritime Organization's International Ship and Port Facility Security code (ISPS) mirrors the MTSA in that it provides a framework of requirements without stipulating specific standards for satisfying those requirements. Ships and port facilities must have security plans, security officers, and certain security equipment but the code leaves it up to each foreign government to provide the specifics. There are no minimum training standards for becoming a "qualified" security officer. There are no mandatory guidelines for what constitutes perimeter security. There are no mandated requirements to govern facility access controls. It is also important to point out that while most ships are in the business of moving cargo, the ISPS code does not address cargo security.

When it comes to port security, the buck essentially stops outside Washington, DC. Since seaports in the United States are locally run operations where port authorities typically play the role of landlord, issuing long-term leases to private companies; it falls largely to those companies to provide for the security of the property they lease.

In the case of Los Angeles, this translates into the security of 7500 acres of facilities that run along 49 miles of waterfront, being provided for by minimum-wage private security guards, and a tiny port police force of under 100 officers. The situation in Long Beach is even worse with only 12 full-time police officers assigned to its 3000 acres of facilities and a small cadre of private guards provided by the port authority and its tenants. The command and control equipment to support a new joint operations center for the few local, state, and federal law enforcement authorities that are assigned to the port will not be in place until 2008. Up to 11,000 independent truck operators have access to the port terminals yet there still is no credentialing system in place to confirm the backgrounds of the drivers. West Coast terminal operators have no way of identifying who is in their facilities at any given moment. In the four years since September 11, 2001, the two cities have received less than $40 million in federal grants to improve the port's physical

security measures. That amount is equivalent to what American taxpayers spend in a single day on domestic airport security.

But the fallout from a terrorist attack on any one of the nation's major commercial seaports would hardly be a local matter. For instance, should al Qaeda or one of its imitator organizations succeed in sinking a large ship in the Long Beach channel, the auto-dependent southern California will literally run out of gas within two weeks. This is because, as Hurricanes Katrina and Rita highlighted, US petroleum refineries are operating at full throttle and their products are consumed almost as quickly as they are made. If the crude oil shipments stop, so too do the refineries and there is no excess capacity or refined fuels to cope with a long term disruption.

But the most serious consequence of a major terrorist attack on America's waterfront is if it involved a weapon of mass destruction smuggled into one of the over nine million 40' cargo containers that entered US seaports in 2005. The September 11, 2001 attacks on New York and Washington, the March 11, 2004 attacks on Madrid, and the July 7, 2005 attacks on London highlight that transport systems have become among the most favored targets for terrorist organizations. Cargo containers have long been exploited to smuggle narcotics, migrants, and stolen property including luxury automobiles. Their vulnerability is highlighted by the billions of dollars in cargo losses derived from theft each year. A typical cargo container that is shipped from Asia will pass through over a dozen transportation waypoints before it is loaded on a ship destined for the United States. Most are "secured" only with a fifty-cent lead seal passed through the pad-eyes on the container doors.

It is just a question of time before terrorists with potentially more destructive weapons breach the superficial security measures that have been put in place to protect the ports, the ships, and the millions of intermodal containers that link global producers to consumers. Should that breach involve a "dirty bomb," the United States and other states will likely raise the port security alert system to its highest level while investigators sort out what happened and establish whether or not a follow-on attack is likely. Multiple port closures in the United States and elsewhere would quickly throw this system into chaos. Container ships already destined for the United States would be stuck in anchorages unable to unload their cargo. Ships would be delayed in overseas loading ports as the maritime industry and their customers try to sort out how to redirect cargo. Marine terminals would have to close their gates to all incoming containers since they would have no place to store them. Trucks and trains would be stuck outside the terminal with no place to go. If they are carrying perishable goods, the cargo would perish. Also, the trucks and trains would not be able to re-circulate to pick up new shipments until they could get rid of the old ones. Goods for export would pile at factory loading docks with no place to go. Imports to support "just-in-time" deliveries would be no shows and soon factories would be idled and retailers' shelves would go bare.

In short, a catastrophic terrorist event involving the intermodal transportation system could well lead to unprecedented disruption to the global trade system. In economic terms, the costs associated with managing the attack's aftermath will substantially dwarf

the actual destruction from the terrorist event itself. Those costs will be borne internationally which is why transportation and trade security must be not only a U.S. Homeland Security priority, but an urgent global priority.

As grave as this threat is, in our fifth year since the 9/11 attacks, there still are no minimum federal standards for access control, perimeter control, electronic surveillance, guards, and communications. State and local port authorities have not been able to make any significant progress towards improving the state of security within their ports. This is largely because ports face a competitive environment where they must make significant capital investments to improve the commercial operations in order to retain or attract shipping lines. It they divert funds away from capital improvements to pay for added security they may face a decline in vessel traffic that reduces their revenues. If they try to pass along increased security costs to their private tenets, those tenets may decide to move to a lower cost neighboring port. In short, in the absence of a level national playing field, U.S. port authorities have been reluctant to make major new investments in security.

The MTSA mandates that ships approaching U.S. waters be equipped with an Automatic Identification System (AIS). However the system the Coast Guard is putting in place is largely a line-of-sight system with a range of about 20 miles. This provides very little time to respond before the ship is detected. Since it is unlikely that Coast Guard patrol vessels would routinely be available to respond to the arrival of a rogue vessel, that vessel could inflict substantial harm long before the means could be mustered to forcibly stop it.

The Coast Guard has in place a requirement that all vessels approaching U.S. ports provide notification of the vessel's last five ports of call, its cargo, and crew members 96 hours before arrival. But it is essentially an honor system since the Coast Guard has no way of confirming when a vessel is 96 hours away, if it is accurately reporting its ports of call and cargo, or if it does not leave any names off its crew list.

At the port of loading, a port facility is supposed to operate in compliance with the ISPS code. MTSA requires that the Coast Guard carry out assessments of overseas ports to ensure they are compliant with the code. However, the agency only has a total of 13 International Port Security Liaison Officers (IPSLO) to cover all of Europe, the Middle East, Africa, Latin America and the Caribbean. There are only another half a dozen liaison officers available to do this for Asia. Presumably these inspectors should know something about port security, be familiar with commercial port operations, and understand the local circumstances, but there is no formal training program in place to develop all of these skills. A single country like Brazil may have over 25 ports, but a typical country assessment visit will involve a 2-3 day country trip and include a visit to just one port.

A Coast Guard inspector visiting an overseas port will likely find that he is following a well worn path. A foreign port could have hosted a Naval Criminal Investigative Service (NCIS) visit. Its terminals may have been subjected to a security audit by U.S. companies under the Customs Trade Partnership Against Terrorism Program. There

could be a team of U.S. customs inspectors operating in the port as a part of the Container Security Initiative. The port may have hosted a visit by the State Department's Export Control, and Related Border Security Assistance (EXBS) program and the Energy's Department's Second Line of Defense & Megaports programs. It is unlikely that any of these visits will have involved interagency coordination in advance.

Under the Container Security Initiative protocol, customs agents will be working with their counterparts to target "high-risk" containers. That determination will be made by examining cargo manifests which must be submitted electronically to CBP 24 hours before it is loaded aboard a ship destined for the United States. But the cargo manifest is notoriously error prone and general and will not even include information such as where the container originally loaded.

In short, the flurry of U.S. government initiatives since 9/11 may create the impression that substantial progress is being made in securing the global trade and transportation system. Unfortunately, all of this activity should not be confused with real capability. For one thing, the approach has been a piecemeal one, with each agency pursuing its signature program or programs with little regard for the other initiatives. There are also vast disparities in the resources that the agencies have been allocated. Then there is the issue of very weak intelligence that underpins the agency's assessments of risk. Further, in an effort to secure funding and public support, agency heads and the White House have oversold the contributions these new initiatives are making towards addressing a very complicated and high-stake challenge. Against a backdrop of inflated and unrealistic expectations, the public will be highly skeptical of official assurances in the aftermath of a terrorist attack involving the intermodal transportation system.

We can do better. With relatively modest investments and a bit of ingenuity, the international intermodal system can have credible security while simultaneously improving their efficiency and reliability. What is required are a series of measures that collectively enhance visibility and accountability within global supply chains.

As a starting point, the United States should work with the Association of Southeast Asian Nations (ASEAN) and the European Union (EU) in authorizing third parties to conduct validation audits of the security protocols contained in the International Ship and Port Facility Security Code and the World Customs Organization's new framework for security and trade facilitation. The companies carrying out these inspections should be required to post a bond as a guarantor against substandard performance and be provided with appropriate liability protections should good-faith efforts prove insufficient to prevent a security breech. A multilateral auditing organization made up of experienced inspectors and modeled on the International Atomic Energy Commission should be created to periodically audit the third party auditors. This organization also should be charged with investigating major incidents and when appropriate, recommend changes to established security protocols.

To minimize the risk that containers will be targeted by terrorist organizations between the factory and a loading port, Washington should embrace and actively promote the

widespread adoption of a novel container security project being sponsored by the Container Terminal Operators Association (CTOA) of Hong Kong. Starting in late 2004, every container arriving at two of the truck gates in two of the busiest marine terminals in the world are, at average speeds of 15 kph, passing through a gamma ray machine to scan its contents, a radiation portal to record the levels of radioactivity found within the container, and optical character recognition cameras which photograph the number painted on the top, back, and two sides of the container. These scanned images, radiation profiles, and digital photos are then being stored in a database for customs authorities to immediately access if and when they want.

One of the benefits of the Hong Kong approach to container inspection is that it can help identify shielded objects that a radiation portal might not pick up and help to resolve a false alarm for benign shipments that have naturally occurring radiation levels. A dirty bomb wrapped in lead may not set off the alarm of a radiation detector, but a gamma image would identify it as a dense object with a suspicious shape in a shipment of sneakers. Alternatively, a radiation portal might register an alarm when examining benign objects like ceramic tiles but by capturing a scanned image at the same time it will be possible to identify the shape of the materials is consistent with what is advertised on the cargo manifest. In this case, the container would not require an additional inspection, thereby reducing the amount of cargo that is pulled from the terminals under the CSI protocol. This in turn would reduce the risk that a container will miss its voyage because of the difficulty in getting it back from the inspection facility in time to be reentered into the outbound vessel's loading plan.

The way that CBP could best make use of the non-intrusive inspection data collected by the system being piloted in Hong Kong is tie the amount of images that they examine to the alert level set under the ISPS protocol. Under Level 1 or the normal alert level, customs inspectors would examine the data as a primary screen only for the high-risk containers they have targeted for inspection using their current algorithm, plus a random sampling of other containers. Under Level 2, they would double or triple the number of containers they look at by using their same risk-based formulation, expanding the pool of inspected containers by lowering the targeting floor by several notches and conducting more random inspections. This will essentially require their surging more inspectors to examine these extra images during the period of heightened alert. In the worst case, under Level 3—which would likely be set after a major terrorist incident—CBP would have to surge enough people to examine every container. This might seem overwhelming at first glance, but even if they took no advantage of software-assisted inspection tools and did the 5-minute manual manipulation of a image that field inspectors currently do, with 26,000 containers arriving in U.S. ports each day, this would require 2170 man-hours per day, or roughly 300 inspectors to examine—not an impossible task for the presumably limited window of time the country would be operating under at Level 3.

In addition to a sustained and systematic effort to bolster the security of the global intermodal transportation system by advancing the use of NII equipment in overseas ports, the White House and Congress must simultaneously invest in securing America's neglected waterfront. There are seven things that must be done right away.

First, over the next 18 months, the Department of Defense must work closely with the U.S. Coast Guard, now part of the Department of Homeland Security, and with local authorities in organizing and participating in exercises that involve simulated attacks on the nation's largest commercial seaports. The training should focus on identifying what is required to quickly restore the operations of the port in the aftermath of a successful attack. These exercises and planning efforts must be a joint DoD-DHS effort, and should also include international maritime industry observers who will be affected by a major U.S. port closure as well and will need to take the lead on making the appropriate near-term adjustments to reduce the risk of a system failure.

Second, DoD needs to take the lead on funding and setting up joint operations centers in all major U.S. commercial ports: to outfit them with advanced information and communications technology that support surveillance and data sharing, and to provide the necessary training to the local, state, and federal agency participants. The resources and skill sets to accomplish this is concentrated within the national security community. It would be too costly and time consuming to try and develop these capabilities without the support of the military. This should be completed by 2007.

Third, the U.S. Navy should reposition one of its two salvage ships in Norfolk, Virginia to the West Coast and take the lead in drawing up commercial salvage contracts to support domestic harbor clearance. Over the next five years, the Navy should double its salvage fleet from four vessels to eight, and base two of them on the West Coast, two on the Gulf Coast, and two on the East Coast. The remaining two can be deployed overseas to support navy operations.

Fourth, the National Oceanographic and Atmospheric Administration (NOAA) hydrographic research vessels should receiving additional funding to complete bottom surveys of the all the major U.S. commercial seaports. This baseline information is indispensable in quickly spotting mines should an adversary deploy them. Without it, the centuries of junk that lay on the floors of most harbors have to be examined by divers to determine if they pose a risk. This post-mining examination could take many weeks or even months in the absence of current bottom survey data.

Fifth, the Coast Guard needs to see a doubling to $2.0 billion of the annual funding to replace its ancient fleet of vessels and aircraft, and to bring its command and control capabilities into the 21st century. Many of its cutters, helicopters, and planes are operating long beyond their anticipated service life and are routinely experiencing major casualties. Under the current delivery schedule, it will be 20-25 years before it has the kind of assets it needs today to perform its mission. This could leave a two-decade gap in capability as the existing fleet becomes too decrepit and dangerous to operate.

Sixth, Congress should authorize the reallocation of all the duties and fees that are collected in seaports to go back into the ports to support security upgrades and infrastructure improvements. Currently, ports are the only transportation sector where the federal government is parasitic. That is, unlike airports and highways, the federal treasury takes more money away than its returns. According to the Coast Guard, seaports need to invest upwards

of $5 billion to put in place minimal access control and physical security measures. Neither the ports nor their city or state governments have those kinds of resources.

Finally, the Customs and Border Protection Agency should receive $20 million in additional funding to expand the information technology capabilities and staffing at its national targeting center so that it can manage the NII scanning data collected in overseas terminals.

Against this backdrop, it should come as no surprise that my assessment of the national security implications of the DP World purchase of Peninsular and Orient Navigations systems and the leases to five containers terminals on the East Coast and New Orleans is that this commercial transaction will not *qualitatively* effect the overall state of global and American maritime transportation security. Stated differently, should a U.S. company assume control of these terminal operations tomorrow, it would not qualitatively improve our security. This is because the problem is less about who owns and operates U.S. container terminals than it is that we simply have not addressed far more serious supply chain, maritime, and port security issues that would dramatically reduce the terrorist risk to our homeland.

In the end, as our dependency on global trade grows and the catastrophic terrorist threat persists, the White House and Congress must start acting as though our commercial seaports are the critical national security assets they are. There should be fewer more urgent priorities than making sure America's ports and the transportation system, responsible for moving the overwhelming majority of world trade, possess adequate capacity, redundancy, and resiliency to meet the daunting challenges that lie ahead.

Thank you and I look forward to responding to your questions.

---

**Stephen Flynn is the author of *America the Vulnerable*. He is currently writing a new book to be published by Random House in Fall 2006 entitled, *The Edge of Disaster: Catastrophic Storms, Terror, and American Recklessness*. He is the inaugural occupant of the Jeane J. Kirkpatrick Chair in National Security Studies at the Council on Foreign Relations. Dr. Flynn served as Director and principal author for the task force report "*America: Still Unprepared—Still in Danger*," co-chaired by former Senators Gary Hart and Warren Rudman. Since 9/11 he has provided congressional testimony on homeland security matters on seventeen occasions. He spent twenty years as a commissioned officer in the U.S. Coast Guard including two commands at sea, served in the White House Military Office during the George H.W. Bush administration, and was director for Global Issues on the National Security Council staff during the Clinton administration. He holds a Ph.D. and M.A.L.D. from the Fletcher School of Law and Diplomacy and a B.S. from the U.S. Coast Guard Academy.**